Keywords: intelligent building, cyber security, building automation, threats, cyber physical systems

Abstract

The concept of an intelligent building has existed for over 30 years and is seen as a solution to a number of economic and environmental problems. Intelligent buildings are often seen as a means of improving the energy efficiency of the built environment. However, they are increasingly being promoted as a means of improving the operational efficiency of buildings, providing enhanced building and personal security, and improving the availability of management information to support better and quicker decision making. The potential cyber security risks inherent in the adoption of intelligent buildings are rarely discussed.

1 Introduction

The potential demand for more intelligent buildings is a response to societal pressures to reduce the impact of buildings on the natural environment, for example, through more efficient use of natural resources in the construction, maintenance and operation of buildings, and the ability to make efficient use of space across a building’s lifecycle. A particular target for this increased efficiency is use of technology to reduce energy consumption. From a building owner or occupier perspective, whilst resource efficiency is important, the expectation is that an intelligent building will provide a degree of automation allowing flexible use of the accommodation and providing tools or applications which support the occupation and management of the space.

To deliver intelligent solutions which improve the efficiency of the building and meet owner and users aspirations regarding the use of the space, there has been pressure to integrate systems. There is also a trend to make increasing use of a wide range of building sensors to acquire occupancy and usage information. Associated with these developments is an increasing use of the Internet to exchange information with third parties and deliver externally hosted services. This integration and connectivity is not without risk, as it exposes the owners and occupants to a variety of cyber security threats.

As noted by Fisk [1], the intelligent building community might protest that there have been no significant successful reported attacks on building management systems (BMS) over the 40 years that the technology has been deployed. This is potentially a complacent view as a range of complex threats are rapidly developing from increasingly sophisticated threat actors.

The first part of this article examines what is meant by an intelligent building and how from a cyber security perspective the convergence of technologies and integration of systems creates vulnerabilities. It then reviews how cyber security affects the built environment, examining the nature of some of the threats and identifying some key management challenges. The article includes a case study examining these issues in the context of an international transport terminal. It then discusses some of the management challenges that need to be addressed to reduce cyber security threats to the built environment.

2 What is an intelligent building?

2.1 Background

The concept of intelligent buildings is not new. Clements-Croome [2] notes that the term ‘intelligent building’ was first used in the United States in the early 1980’s and that a definition given by the Intelligent Building Institution in Washington was: “An intelligent building is one which integrates various systems to effectively manage resources in a coordinated mode to maximise: technical performance; investment and operating cost savings; flexibility”. The innovative idea of a building operating with a converged technical infrastructure as a ‘computer integrated building’ was first proposed by DEGW/Teknibank [3], as illustrated in Figure 1. Putting their pioneering work into perspective, this proposal for the convergence of systems based on an IP-network infrastructure was published before the Ethernet (TCP/IP) was generally accepted as a universal protocol for communications, before the creation of the Internet as we now know it, and several years before any commercial trading took place on the Internet.

Since this early work by DEGW and Teknibank, there have been a number of definitions of what is meant by the term intelligent building. For example Ehrlich [4] defines it as “use of technology and process to create a building that is safer and more productive for its occupants and more operationally efficient for its owners”. This definition reflects the needs of owners and occupiers, but does not explicitly address the environment. Another definition is offered by Harrison [5], an intelligent building “provides a responsive, effective and
supportive intelligent environment within which the organisation can achieve its business objectives“.

Underpinning these definitions is the Integration Pyramid model and increasingly through IP convergence, the integration of the multi-function building and user systems with business systems.

The range of systems that may typically be integrated within an intelligent building is illustrated in Figure 2 [6]. For a building to be intelligent it is not essential for all of these systems to be present, integrated or to share a common infrastructure. It is the systems integration and sharing of data to deliver additional functionality that creates an intelligent building.

2.2 Intelligent building case study – Airport Terminal

A consequence of the continuing growth of air transport, e.g. 65% increase in global scheduled passenger volumes over the last decade [7], are significant economic and environmental pressures on the owners and operators of international air terminals. Airports need to handle these increasing passenger volumes safely and securely, whilst reducing the cost of ownership of the terminals and their environmental impact. The transport industry is addressing these problems through the use of innovative IT-enabled solutions, allowing them to achieve energy savings and to increase passenger capacity of terminals.

Modern airport terminals are now typically delivered with a converged IP-based network infrastructure [8], based on a common cabling system. This networking infrastructure is required to support a diverse range of operational, business and facilities management systems as illustrated in Figure 3. Economic pressures for operational efficiencies has created a demand for increased integration of applications, which allows streamlined handling of data and eliminates the need for data re-entry thus reducing risks of errors.

By adopting common, compatible physical distribution and networking layers in the architecture, as shown in Figure 3, the systems delivering applications use industry standards protocols to communicate between any distributed elements and via the systems integration layer, with one another. For example from a central control room, an operator may be able to control landside systems using dynamic signage to provide directions for passenger vehicle traffic. Using sensors in parking bays, the system may then automatically indicate to drivers the location of available parking spaces. If a customer has pre-booked parking, a space may be allocated and barrier access controlled using CCTV and ANPR systems. The security of the terminal and its adjacent highways and parking areas will typically be overseen from a security control room.
using IP-based CCTV and security systems. From a security perspective ANPR may be used for the identification and monitoring of suspicious vehicles in the public highway and terminal approaches. From a safety perspective tampering with or failure of signage on vehicle routes could cause vehicle accidents and injuries to pedestrians.

Within a terminal sharing of passenger data between systems may allow Internet check-in, make baggage handling more efficient, and allow the customs and border security staff to monitor arrivals and processing of passengers. In addition to the use of IT systems to provide travellers and visitors to the terminal with up to date arrivals and departures information, customers increasingly expect to have Internet access with public access in terminals and Wi-Fi readily available both land and air side.

In the airport terminal, a common infrastructure will typically be used to support a range of network-based services [8], including: CCTV; access control systems; fire alarms; badging systems; computer aided dispatch; incident management; and visa and passport control. Given an operational need to flexibly manage terminal accommodation, particularly in public areas, the building management systems, internal signage systems and access control systems are all likely to use this common infrastructure. Through appropriate systems integration this allows passenger flow in corridors and stairways to be switched between arrivals and departure areas to suit operational needs of the airport. From an environmental perspective this integration may also allow the heating, lighting and air conditioning of areas to be reduced when they are not in use by passengers.

This integrated infrastructure will also be used to support the operation of the terminal from a business perspective, e.g. to provide HR services, staff email and internet access, asset management, etc. There may be some integration of business systems and security systems to enable flexible management and allocation of staff, based on their skills and security clearances.

This case study illustrates how an intelligent building may depend on a diverse range of systems, using common commercially available technologies. The integration and interaction of these systems increases the probability that the design will include significant and potentially unforeseen cyber security vulnerabilities.

3 Cyber security in the built environment

3.1 Defining cyber security

In the built environment, it is important to recognise that cyber security affects more than the IP-based networks in a building. An internationally agreed definition [9] which recognises this broader scope of cyber security is "the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user’s assets". This definition refers to the “cyber environment” (or cyberspace), which effectively comprises the interconnected networks of electronic, computer-based and wireless systems. The definition also refers to "organization and user’s assets", which effectively includes all connected computing devices, personnel, infrastructure, applications, services, telecommunication systems, and the totality of transmitted, processed and/or stored data and information in the cyber environment. In protecting the ‘cyber environment’ we also need to address the safety of those that could be affected by systems failure or malfunction.

Cyber security has developed from the discipline of information security, which was based on three core principles [10]:

- Confidentiality – which encompasses privacy, and the control and authorisation of access to data or information, and any ability to process, modify or delete data or information;
- Integrity – which addresses the trustworthiness of the data or information storage, the authenticity to data and results, and the safe operation of electronic systems; and
- Availability – the availability of the systems and associated business functions when needed.

These principles are commonly referred to as the CIA triad. When considering the security of corporate IT systems, the order of triad is often seen as reflecting the priority of these attribute. This contrasts with the needs of control systems, e.g. those used for building management and security where availability and then integrity typically have a higher priority than confidentiality. This combination of availability and integrity may be considered as resilience, i.e. the ability to adapt and respond to disruption and maintain functionality.

3.2. Application in the built environment

In an intelligent building, the convergence of infrastructure technologies (e.g. networks and sensors), and systems integration can create significantly increased cyber security risks. Without careful implementation, the complexity inherent in this ‘system of systems’ may result in the application of the ‘Law of Unintended Consequences’ [11].

The complexity of applying cyber security to systems in the built environment inevitably becomes more complex as the degree of integration between systems increases. For example sensors within a building may be used for multiple purposes. The output from a CCTV camera may be used by:

- an operator to monitor and observe individuals in the building;
- security systems to detect suspicious objects;
- alarm systems to detect movement in an area which is currently out of bounds or not in use;
- building systems to save energy by restricting or shutting down environmental conditioning systems in unoccupied areas.
These applications will require feeds of digital data to systems with different security profiles and sensitivities, some of which may be located outside the terminal building. Failure to implement adequate cyber security measures could result in data loss, with images being viewed by unauthorised individuals, or even broadcast over the Internet. The exposure of the CCTV feeds may cause serious reputational damage to the terminal operator, particularly if individual passengers can be identified.

From a cyber security perspective, the greatest risk to an intelligent building is likely to be from the potential impact on the building control systems, in particular any loss of view or loss of control. Building management systems are typically designed to operate on their own dedicated network with security providing access control at operator workstations, but little or no security implemented between control computers and sensors or the systems being controlled. Unauthorised direct access to this network could allow a user to interfere with building systems, resulting in loss of control or view and causing significant safety or security issues, e.g. an inability to shutdown mechanical equipment should a life threatening incident occur. Similarly, unauthorised modification of data could undermine systems integrity causing operator errors or loss of control. These situations could arise in an intelligent building if there is inadequate security between any networks used by office staff and/or the public, and the building management network.

4 Threats to intelligent buildings

4.1 Source and nature of threats

Cyber security threats to an intelligent building will emanate from four types of threat agent: malicious outsiders; malicious insiders; non-malicious insiders; and nature [12]. The threats from malicious agents may be indiscriminate, such as distribution of malware or viruses, or targeted attacks attempting to compromise, disrupt or damage specific systems. Threats from nature relate to damage or interference to buildings systems, arising from solar, weather, animal or insect threat agents.

The malicious threats will typically originate from one of the following groups [13]:
- Sole activists
- Activist groups
- Competitors
- Organised crime
- Terrorists
- Proxy terror threat agents with nation state support
- Nation states

The above list is ordered to reflect the increasing capacity for damage and potential sophistication of threats originating from the threat group. The nature of malicious threats will vary depending on the motivation and objectives of a threat group. Their intent may be to cause commercial or reputational harm, to steal intellectual property or to simply cause disruption.

The airport terminal described earlier in this article could be a target of malicious cyber security attacks by any of the above threat groups. Their intent may be to disable systems for terrorist or criminal purposes. For example, were a robbery to occur today, like the one which occurred in November 1983 [14] - involving the Brink's-MAT warehouse at Heathrow Airport, London, it is likely that the perpetrators might have used cyber security attacks in their planning or execution of the robbery.

4.2 Assessing vulnerabilities

To identify and address potential cyber security vulnerabilities a risk management cycle [15] will typically be used as illustrated in Figure 4. The objective of using this cycle is to analyse potential threats, allowing development of proportionate safeguards to enable suitable mitigation to be put in place. When considering cyber security related risks affecting an intelligent building, the owner/operator can choose to avoid the risk, to reduce the risk, to share it or to retain it.

In an international airport terminal maintaining security of the air-side/ground-side interface is critical for effective immigration and customs control and to deter air transport related terrorism. It is essential that availability and integrity of these systems are maintained. The design of new security systems (access control, CCTV, and badging systems) are TCP/IP network based. If for example, following an assessment of vulnerabilities, a terminal owner/operator may determine that the following cyber security vulnerabilities should to be addressed as they could lead to physical security breaches:

- the potential for loss of systems availability due to mains power failure;
- the use of wireless networking would be susceptible to jamming or interference thus affecting network availability;
- the risk of unauthorised access and data corruption if the security systems infrastructure is not adequately protected where is passes through public areas. This
may affect both confidentiality (access control) and integrity (of systems data).

In assessing risks associated with these vulnerabilities, the terminal operator can decide to avoid the risk through the following measures:

- to prevent power loss, supply these systems with electricity from an uninterruptible power supply (UPS) supported by back-up generators;
- To only use cabled networks thereby eliminating the risks of jamming or RF interference;
- To avoid unauthorised access in public areas, the cables may be routed via secure distribution ducts preventing physical access to the cable distribution system. Alternatively, the terminal owner/operator may choose to implement appropriate network security measures (e.g. firewalls, intrusion detection systems, etc.) to maintain flexibility whilst reducing risk of attacks from outside the secure area.

5 Management challenges

Throughout a building’s lifecycle those responsible for managing it will face a number of challenges which affect its cyber security. During the specification and design stages an important issue may be to protect investment in the intellectual property rights (IPR). This may be of particular significant where a design involves proprietary or innovative features or techniques.

The use of Building Information Modelling (BIM) [16] potentially introduces a number of cyber security risks, including:

- the potential for loss or unauthorised access to sensitive designs;
- management of data, including configuration management;
- the exposure of site security vulnerabilities allowing vulnerability reconnaissance without need for physical access to the site or building.

The latter point may be a particular issue for sensitive buildings such as banks, prisons, military establishments and sites supporting the critical national infrastructure.

Building security has traditionally involved creating and maintaining a secure physical perimeter. This typically involves minimising and controlling the points of entry and egress. The interconnection of business and building systems with the Internet significantly increases the attack surface for any building, as a potential intruder now has both physical and logical avenues to attack. Internet connectivity also removes the need for an attacker to be near or inside a building or site. This challenge is particularly significant where a building’s security and alarm systems operate over the building’s IT infrastructure. A failure to adequately secure these systems could allow a cyber security attack to remotely disable or disrupt them.

It is essential to recognise that insiders, i.e. those with authorised access to the building and its systems, can be a significant cyber security threat. An attack from a knowledgeable and malicious insider could be particularly devastating as the attacker may have a good understanding of which systems to attack or disable. However negligent or careless insiders can also cause significant disruption or damage, for example by plugging malware infected removable media into a building or business system. Failures by insiders to properly execute security procedures, to monitor alarms and system logs or correctly configure/maintain security systems and access control will significantly increase the security vulnerabilities.

With the increasing convergence of building and business systems, and the complexity associated with this systems integration, there is an increased need for greater collaboration between IT and facilities management teams. For example these teams need to collaborate about the management of interfaces between their systems and the security measures in place to protect them. Without this collaboration there is a risk that the business systems and their interfaces may be used to mount an attack on the building systems or vice versa. Collaboration will require team members to have an appreciation of how different types of system work and may be protected. This is important as some techniques used to protect an administrative system may be inappropriate or not feasible on real-time control systems.

Another potentially significant management challenge is the on-going systems engineering and management throughout the building lifecycle. A significant difference between business and building systems is their typical lifetimes. A business system might typically be operational for 3 to 5 years, whereas a building system may have a lifetime of between 5 and 20 years [17]. The implication of these differing lifetimes is that over a building’s operational lifecycle there will be a number of changes as business systems become obsolete and are replaced. The impact of these changes will need to be assessed and given increasing complexity of intelligent buildings this may require in depth systems engineering knowledge of all affected systems.

6 Discussion

This article has examined the development of intelligent buildings. Since the prescient prediction by DEGW and Teknibank in 1992 [18], their vision of an intelligent building is being realised through infrastructure convergence. Current economic and environmental pressures encourage development of intelligent buildings to address these societal needs. The current generation of intelligent buildings are potentially an important stepping stone towards innovations such as smart cities and the smart grid.

Unfortunately the elements of a building which make them smart or intelligent also create significant vulnerabilities. Whilst there are few reports of attacks on buildings systems [19], the increasing incidents involving malware such as Stuxnet [20], Flame [21] and Duqu [22] suggest that it is only
The continuing rapid development of technology and to cyber security incidents. Possibly the greatest challenge will be to achieve a single team solution to maintenance and operation of both business and building systems. This situation will be further complicated if the current cultural, contractual and skills differences between these teams are not addressed. For example it is common practice for organisations to outsource the majority of their facilities management activities, whereas the level of outsourcing within a corporate IT department can vary across a wide spectrum. In an intelligent building a matrix of contracts may therefore exist with a number of contractors sharing responsibility for the overall cyber security of the building. This can significantly increase the complexity of maintaining adequate defences and responding to cyber security incidents.

The continuing rapid development of technology and solutions will pose another significant challenge for the building manager, e.g. the use of ‘cloud services’. The airport terminal referred to in the case study in this article is a typical building where cloud services may be used for the business systems. The consequence of failure of these services could be disruption to the business operations, e.g. checking-in of passengers. Whilst disruptive, this is unlikely to affect the health or safety of terminal users. However building systems suppliers [23] are developing solutions employing ‘cloud services’ for building management. If these building services are delivered via ‘cloud services’ are critical to the safe and secure operation of the building then any interruption to these externally hosted services or connectivity to them could seriously disrupt the use of the building. From a resilience and cyber security perspective, availability and integrity of these ‘cloud services’ then becomes critical to the safety and security of terminal users.

The increasing use of BIM, a transformational initiative within the architecture, construction and engineering (ACE) industries has significant cyber security implications. As these industries move from their current use of BIM at Level 2 maturity (i.e. managed CAD in 2D or 3D format) to Level 3 (iBIM – a managed 3D environment), cyber security risks will increase unless appropriate steps are taken. Increased sharing of electronic data between companies in the building design and construction supply chains has implications for both the security of the building models and due to the connectivity to the organisations involved. These problems do not cease on handover of a building to the owner as BIM models are intended to be used by an owner and their facility manager to support the on-going management and maintenance of the building. The parties involved in design delivery and operation of a building will need to consider how the integrity of the model can be assured throughout a building’s lifecycle.

To address the issues outlined in this article, there is a need for those involved in the design, construction and operation of intelligent buildings to have a good awareness of cyber security issues. Attempting to address the issues retrospectively on handover of a new building is rarely satisfactory and may involve significant rework and cost, whilst failing to deliver a resilient solution. Cyber security is as critical to intelligent buildings as disciplines such as structural and fire engineering are to multi-storey buildings. It will need to become part of the routine risk assessment process for all building projects, just as issues such as ground conditions, earthquake risk, etc. are assessed based on the building location.

Applying appropriate systems and software engineering techniques to the design of the cyber environment is an essential first step. A number of these techniques are covered in the “20 Critical Controls” [24], which should be a reasonable starting point for the cyber security protection of any intelligent building. There is a significant body of knowledge related to the development of trustworthy software [25] and lessons that can be learned from the design and implementation of safety-critical systems.

7 Conclusions

With increasing use of network and information technology to deliver smart or intelligent buildings there are a number of technical and management challenges to address. The use of these technologies potentially offers significant benefit to society, but should be balanced with the inherent cyber security risks. If these risks are not addressed throughout a building’s lifecycle the consequences could be serious health and safety issues.

There is a considerable body of knowledge available regarding systems and software engineering practice and their application to safety-critical systems. Applying this knowledge and combining it with best practice cyber security guidance such as the “20 Critical Controls” could significantly reduce the vulnerability of intelligent buildings. The IET developed briefing document, referred to in this article is intended to help raise awareness.

The ACE industries urgently need to raise cyber security awareness, particularly with their increasing dependence on network and IT solutions. This awareness should cover the full building lifecycle and will need to be accompanied by appropriate skills level in those involved.

Acknowledgements

The author wishes to acknowledge the support received from the UK Centre for Protection of National Infrastructure (CPNI) during the development of a report on Resilience and Cyber Security of Technology in the Built Environment [6].
References


